

Módulo 13:**ANILLO DE POLINOMIOS**

En este módulo nos referiremos al anillo de polinomios de cualquier cuerpo. En esta estructura se aplican gran parte de las propiedades y teoremas de los capítulos anteriores, destacando uno de los teoremas importantes que hace mención a la extensión a cuerpo, así como otros que nos indican cuando algunos elementos de este anillo son irreducibles, como lo es el criterio de Eisenstein entre otros.

Definición 1: Sea A un anillo, un polinomio $f(x)$ en la indeterminada x , y con coeficientes en A , es la siguiente suma formal infinita.

$$f(x) = a_0 + a_1 \cdot x + \dots + a_n \cdot x^n + \dots = \sum_{i=0}^{\infty} a_i \cdot x^i$$

Con la condición que los $a_i = 0$ salvo para un número finito de valores de i .

Si $a_i = 0$, $\forall i > n$ se anota:

$$f(x) = a_0 + a_1 \cdot x + \dots + a_n \cdot x^n$$

Los $a_i \in A$ son los coeficientes del polinomio

Si $\nexists i > 0$ se cumple que $a_i \neq 0$ el mayor valor de i recibe el nombre de grado del polinomio. Si tal i no existe se dice que el polinomio tiene grado 0.

Ejemplo 1:

$f(x) = a$, con $a \in A$. Luego $f(x)$ tiene grado 0.

Definición 2: Se denota por $A[x]$ al conjunto de los polinomios $f(x)$. En $A[x]$ se define la suma como:

$$\text{Sean } f(x) = a_0 + a_1 \cdot x + \dots + a_n \cdot x^n + \dots$$

$$g(x) = b_0 + b_1 \cdot x + \dots + b_n \cdot x^n + \dots$$

$$\text{Luego } f(x) + g(x) = h(x) = d_0 + d_1 \cdot x + \dots + d_n \cdot x^n + \dots$$

$$\text{Donde } d_n = a_n + b_n, \forall n$$

Observación: $(A[x], +)$ es un grupo abeliano, en efecto:

i) Es cerrada:

Es evidente por definición.

ii) Asociatividad:

Para todo $f(x), g(x), h(x) \in A[x]$ por demostrar que

$$f(x) + [g(x) + h(x)] = [f(x) + g(x)] + h(x)$$

Se tiene que $f(x) + [g(x) + h(x)] =$

$$= f(x) + [b_0 + b_1 \cdot x + \dots + b_n \cdot x^n + \dots + d_0 + d_1 \cdot x + \dots + d_n \cdot x^n + \dots]$$

$$= f(x) + [(b_0 + d_0) + (b_1 + d_1) \cdot x + \dots + (b_n + d_n) \cdot x^n + \dots]$$

donde $u_i = b_i + d_i, \forall i$, luego:

$$f(x) + (u_0 + u_1 \cdot x + \dots + u_n \cdot x^n + \dots) = v_0 + v_1 \cdot x + v_2 \cdot x^2 + \dots + v_n \cdot x^n + \dots$$

con $v_i = a_i + u_i, \forall i$

$$\begin{aligned}
 &= [a_0 + (b_0 + d_0)] + [a_1 + (b_1 + d_1)] \cdot x + \dots + [a_n + (b_n + d_n)] \cdot x^n + \dots \\
 &= [(a_0 + b_0) + d_0] + [(a_1 + b_1) + d_1] \cdot x + \dots + [(a_n + b_n) + d_n] \cdot x^n + \dots \\
 &= (f(x) + g(x)) + h(x)
 \end{aligned}$$

iii) Conmutatividad:

Para todo $f(x), g(x) \in A[x]$ por demostrar que:

$$f(x) + g(x) = g(x) + f(x)$$

Se tiene que:

$$\begin{aligned}
 f(x) + g(x) &= a_0 + a_1 \cdot x + \dots + a_n \cdot x^n + \dots + b_0 + b_1 \cdot x + \dots + b_n \cdot x^n + \dots \\
 &= (a_0 + b_0) + (a_1 + b_1) \cdot x + \dots + (a_n + b_n) \cdot x^n + \dots
 \end{aligned}$$

con $a_0, b_0, a_1, b_1, a_n, b_n \in A$

$$\begin{aligned}
 &= (b_0 + a_0) + (b_1 + a_1) \cdot x + \dots + (b_n + a_n) \cdot x^n + \dots \\
 &= b_0 + b_1 \cdot x + \dots + b_n \cdot x^n + \dots + a_0 + a_1 \cdot x + \dots + a_n \cdot x^n + \dots \\
 &= g(x) + f(x)
 \end{aligned}$$

iii) Elemento Neutro.

Debe existir $f(x) \in A[x]$ para todo $g(x) \in A[x]$ tal que

$$f(x) + g(x) = g(x) + f(x) = g(x)$$

Supongamos que:

$$f(x) + g(x) = g(x), \text{ luego se cumple que:}$$

$$a_0 + a_1 \cdot x + \dots + a_n \cdot x^n + b_0 + b_1 \cdot x + \dots + b_n \cdot x^n = b_0 + b_1 \cdot x + \dots + b_n \cdot x^n + \dots$$

Como $a_i, b_i \in A, \forall i$, luego $a_0 + a_1 \cdot x + \dots + a_n \cdot x^n + \dots = 0$, por lo tanto el neutro en $A[x]$ es $f(x) = 0 = 0 + 0 \cdot x + 0 \cdot x^2 + \dots + 0 \cdot x^n + \dots$

iv) Elemento Inverso

Para todo $f(x) \in A[x]$ debe existir $g(x) \in A[x]$ tal que

$$f(x) + g(x) = g(x) + f(x) = 0$$

Supongamos que:

$$f(x) + g(x) = 0, \text{ esto es:}$$

$$a_0 + a_1 \cdot x + \dots + a_n \cdot x^n + \dots + b_0 + b_1 \cdot x + \dots + b_n \cdot x^n = 0, \text{ es decir,}$$

$$\sum_{i=0}^{\infty} a_i \cdot x^i + \sum_{j=0}^{\infty} b_j \cdot x^j = 0, \text{ con } a_i, b_j \in A, \forall i, j$$

Luego sumando el inverso aditivo de $\sum_{i=0}^{\infty} a_i \cdot x^i$ por la izquierda se tiene:

$$-\sum_{i=0}^{\infty} a_i \cdot x^i + \sum_{i=0}^{\infty} a_i \cdot x^i + \sum_{j=0}^{\infty} b_j \cdot x^j = -\sum_{i=0}^{\infty} a_i \cdot x^i$$

$$\sum_{j=0}^{\infty} b_j \cdot x^j = -\sum_{i=0}^{\infty} a_i \cdot x^i$$

En consecuencia, $g(x) = -f(x)$, ahora si $f(x) = \sum_{i=0}^{\infty} a_i \cdot x^i$ entonces su

inverso es $-f(x) = \sum_{i=0}^{\infty} (-a_i) \cdot x^i$.

En consecuencia de i), ii), iii), iv) y v) $A[x]$ es grupo abeliano.

Definición 3: En $A[x]$ se define el producto como:

Sean $f(x) = \sum_{i=0}^{\infty} a_i \cdot x^i$; $g(x) = \sum_{j=0}^{\infty} b_j \cdot x^j$, luego

$$f(x) \cdot g(x) = \sum_{k=0}^{\infty} d_k \cdot x^k, \text{ con } d_k = \sum_{r=0}^k a_r \cdot b_{k-r}$$

Ejemplo 2:

$$\text{Sean } f(x) = 2 \cdot x^3 + 4 \cdot x^2 - 5 = a_3 \cdot x^3 + a_2 \cdot x^2 - a_0$$

$$g(x) = 6 \cdot x^2 + x = b_2 \cdot x^2 + b_1 \cdot x$$

$$\text{Luego } f(x) \cdot g(x) = (2 \cdot x^3 + 4 \cdot x^2 - 5) \cdot (6 \cdot x^2 + x)$$

$$= 12 \cdot x^5 + 2 \cdot x^4 + 24 \cdot x^4 + 4 \cdot x^3 - 30 \cdot x^2 - 5x$$

$$= 12 \cdot x^5 + 26 \cdot x^4 + 4 \cdot x^3 - 30 \cdot x^2 - 5 \cdot x$$

$$\text{Tenemos que: } f(x) \cdot g(x) = d_0 + d_1 \cdot x + d_2 \cdot x^2 + d_3 \cdot x^3 + d_4 \cdot x^4 + d_5 \cdot x^5$$

$$\text{Ahora, } d_5 = \sum_{r=0}^5 a_r \cdot b_{5-r} = a_0 \cdot b_5 + a_1 \cdot b_4 + a_2 \cdot b_3 + a_3 \cdot b_2 + a_4 \cdot b_1 + a_5 \cdot b_0$$

$$= (-5) \cdot 0 + 0 \cdot 0 + 4 \cdot 0 + 2 \cdot 6 + 0 \cdot 1 + 0 \cdot 0 = 12$$

$$d_4 = \sum_{n=0}^4 a_r \cdot b_{4-r} = \cancel{a_0} \cdot \cancel{b_4}^0 + \cancel{a_1} \cdot \cancel{b_3}^0 + a_2 \cdot b_2 + a_3 \cdot b_1 + \cancel{a_4} \cdot \cancel{b_0}^0$$

$$= 4 \cdot 6 + 2 \cdot 1 = 26$$

$$d_3 = \sum_{r=0}^3 a_r \cdot b_{3-r} = \cancel{a_0} \cdot \cancel{b_3}^0 + \cancel{a_1} \cdot \cancel{b_2}^0 + a_2 \cdot b_1 + \cancel{a_3} \cdot \cancel{b_0}^0$$

$$= 4 \cdot 1 = 4$$

$$d_2 = \sum_{r=0}^2 a_r \cdot b_{2-r} = a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0$$

$$= (-5) \cdot 6 = -30$$

$$d_1 = \sum_{r=0}^1 a_r \cdot b_{1-r} = a_0 \cdot b_1 + a_1 \cdot b_0$$

$$= -5$$

$$d_0 = \sum_{r=0}^0 a_r \cdot b_{0-r} = a_0 \cdot b_0$$

$$= 0$$

$$\text{Por lo tanto } f(x) \cdot g(x) = \sum_{i=0}^{\infty} d_i \cdot x^i = 12 \cdot x^5 + 26 \cdot x^4 + 4 \cdot x^3 - 30 \cdot x^2 - 5 \cdot x$$

Nota: Anotaremos por gr al grado de un polinomio.

Del ejemplo anterior podemos decir:

$$gr(f(x) \cdot g(x)) = 5 = 3 + 2 = gr(f(x)) + gr(g(x))$$

es válido $\forall f(x), g(x) \in A[x]$ con $f(x), g(x) \neq 0$

Por otro lado podemos decir que:

$$gr(f(x) + g(x)) \leq \max(gr(g(x)), gr(f(x)))$$

Observación: $(A[x], +, \cdot)$ es un anillo, en efecto:

De lo anterior podemos decir que $(A[x], +)$ es Grupo Abelianiano.

Ahora solo basta demostrar la asociatividad con la segunda operación y la distributividad de la segunda operación con respecto a la primera, esto es:

i) Asociatividad:

Para todo $f(x), g(x), h(x) \in A[x]$ por demostrar que:

$$f(x) \cdot [g(x) \cdot h(x)] = [f(x) \cdot g(x)] \cdot h(x)$$

$$\begin{aligned}
 & \left[\left(\sum_{i=0}^{\infty} a_i \cdot x^i \right) \left(\sum_{j=0}^{\infty} b_j \cdot x^j \right) \right] \left(\sum_{k=0}^{\infty} c_k \cdot x^k \right) = \left(\sum_{i=0}^{\infty} a_i \cdot x^i \right) \left[\left(\sum_{j=0}^{\infty} b_j \cdot x^j \right) \left(\sum_{k=0}^{\infty} c_k \cdot x^k \right) \right] \\
 & = \left(\sum_{i=0}^{\infty} a_i \cdot x^i \right) \cdot \left(\sum_{n=0}^{\infty} \left(\sum_{r=0}^n b_r \cdot c_{n-r} \right) \cdot x^n \right) \\
 & = \sum_{s=0}^{\infty} \left(\sum_{n=0}^s a_{s-n} \left(\sum_{r=0}^n b_r \cdot c_{n-r} \right) \right) \cdot x^s \\
 & = \sum_{s=0}^{\infty} \left(\sum_{i+j+k=s} a_i \cdot b_j \cdot c_k \right) \cdot x^s \\
 & = \sum_{s=0}^{\infty} \left[\sum_{n=0}^s \left(\sum_{i=0}^n a_i \cdot b_{n-i} \right) \cdot c_{s-n} \right] \cdot x^s \\
 & = \left[\sum_{n=0}^{\infty} \left(\sum_{i=0}^{\infty} a_i \cdot b_{n-i} \right) \cdot x^n \right] \left(\sum_{k=0}^{\infty} c_k \cdot x^k \right) \\
 & = \left[\left(\sum_{i=0}^{\infty} a_i \cdot x^i \right) \left(\sum_{j=0}^{\infty} b_j \cdot x^j \right) \right] \left(\sum_{k=0}^{\infty} c_k \cdot x^k \right)
 \end{aligned}$$

ii) Distributividad:

La distributividad se demuestra de manera análoga y queda de ejercicio para el lector.

Observación: De lo anterior podemos decir que $(A[x], +, \cdot)$ es un anillo de polinomios.

Proposiciones: Sea $(A[x], +, \cdot)$ un anillo de polinomios, luego se tiene:

- 1.- Si A es un anillo conmutativo entonces $A[x]$ es conmutativo.
- 2.- Si la identidad de A es 1 entonces la identidad de $A[x]$ es $f(x) = 1$.
- 3.- Si A es un Dominio de Integridad entonces $A[x]$ es un Dominio de Integridad.

Demostración 1)

Dados $f(x), g(x) \in A[x]$ por demostrar que $f(x) \cdot g(x) = g(x) \cdot f(x)$

Se tiene: $f(x) = a_0 + a_1 \cdot x + \dots + a_n \cdot x^n + \dots$ y $g(x) = b_0 + b_1 \cdot x + \dots + b_m \cdot x^m$

Luego, $f(x) \cdot g(x) = c_0 + c_1 \cdot x + \dots + c_s \cdot x^s + \dots$

$g(x) \cdot f(x) = d_0 + d_1 \cdot x + \dots + d_s \cdot x^s + \dots$, con $s = m + n$, pero todo

$$\begin{aligned}
 0 \leq i \leq s, \text{ obtenemos: } & c_i = \sum_{k+j=i}^{\infty} a_k \cdot b_j \\
 & = \sum_{j+k=i}^{\infty} b_j \cdot a_k \\
 & = d_i
 \end{aligned}$$

Luego $f(x) \cdot g(x) = g(x) \cdot f(x)$ por tener todos sus coeficientes iguales.

Demostración 2):

Debe existir $g(x) \in A[x]$ para todo $f(x) \in A[x]$ tal que

$$f(x) \cdot g(x) = g(x) \cdot f(x) = f(x)$$

Supongamos que $f(x) \cdot g(x) = f(x)$, luego se tiene que:

$$\left(\sum_{i=0}^{\infty} a_i \cdot x^i \right) \cdot \left(\sum_{j=0}^{\infty} b_j \cdot x^j \right) = \left(\sum_{i=0}^{\infty} a_i \cdot x^i \right)$$

Como $f(x) \cdot g(x) = \sum_{k=0}^{\infty} d_k \cdot x^k$, con $d_k = \sum_{r=0}^k a_r \cdot b_{k-r}$, entonces,

$$\sum_{k=0}^{\infty} d_k \cdot x^k = \sum_{i=0}^{\infty} a_i \cdot x^i, \text{ esto es:}$$

$$d_0 + d_1 \cdot x + d_2 \cdot x^2 + \dots + d_n \cdot x^n + \dots = a_0 + a_1 \cdot x + a_2 \cdot x^2 + \dots + a_n \cdot x^n + \dots$$

En consecuencia;

$$(a_0 \cdot b_0) + (a_0 \cdot b_1 + a_1 \cdot b_0) \cdot x + (a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0) x^2 + \dots + \\ + \left(\sum_{r=0}^n a_r \cdot b_{n-r} \right) \cdot x^n + \dots = a_0 + a_1 \cdot x + a_2 \cdot x^2 + \dots + a_n \cdot x^n + \dots$$

Por igualdad de polinomios se obtiene:

$$a_0 \cdot b_0 = a_0, \text{ luego } b_0 = 1$$

$$a_0 \cdot b_1 + a_1 \cdot b_0 = a_1, \text{ como } b_0 = 1 \text{ se tiene}$$

$$a_0 \cdot b_1 + a_1 = a_1 \text{ entonces } a_0 \cdot b_1 = 0, \text{ luego } b_1 = 0$$

$$a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0, \text{ como } b_0 = 1 \text{ y } b_1 = 0 \text{ obtenemos}$$

$$a_0 \cdot b_2 + a_2 = a_2 \text{ entonces } a_0 \cdot b_2 = 0, \text{ luego } b_2 = 0$$

Ahora siguiendo análogamente el algoritmo podemos inducir que los demás coeficientes del polinomio $g(x)$ son cero.

Por lo tanto $g(x) = 1 + 0 \cdot x + 0 \cdot x^2 + \dots + 0 \cdot x^n + \dots = 1$, identidad en $A[x]$.

Demostración 3):

Solo basta demostrar que $A[x]$ es sin divisores de cero, es decir si:

Si $f(x) \cdot g(x) = 0$ entonces $f(x) = 0$ ó $g(x) = 0$

o bien, si $f(x) \neq 0$ y $g(x) \neq 0$ entonces $f(x) \cdot g(x) \neq 0$

Sean:

$f(x) = a_0 + a_1 \cdot x + \dots + a_n \cdot x^n$, supongamos que $a_n \neq 0$, $a_i = 0$, $\forall i > n$

$g(x) = b_0 + b_1 \cdot x + \dots + b_m \cdot x^m$, supongamos que $b_m \neq 0$, $b_j = 0$, $\forall j > m$

Debemos demostrar $f(x) \cdot g(x) \neq 0$, luego tenemos;

Si $f(x) \cdot g(x) = h(x) = \sum_{i=0}^{n+m} c_i \cdot x^i$ por demostrar que $c_i \neq 0$, $\forall i$

Esto es,

$$\begin{aligned}
 c_{n+m} &= \sum_{r=0}^{n+m} a_r \cdot b_{n+m-r} = \cancel{a_0 \cdot b_{n+m}^0} + \cancel{a_1 \cdot b_{n+m-1}^0} + \cancel{a_2 \cdot b_{n+m-2}^0} + \dots + \\
 &+ a_n \cdot b_m + \cancel{a_{n+1} \cdot b_{m-1}^0} + \dots + \cancel{a_{n+m} \cdot b_0^0}
 \end{aligned}$$

pero $a_n \cdot b_m \neq 0$, pues $a_n \neq 0$ y $b_m \neq 0$, con $a_n, b_m \in A$ Dominio de Integridad, por lo tanto $c_{n+m} \neq 0$, luego $A[x]$ es sin divisores de cero.

Teorema: Sean F y K dos cuerpos tal que F subcuerpo de K , con $\alpha \in K$, entonces la función: $\phi_\alpha : F[x] \rightarrow K$ tal que $\phi_\alpha(f(x)) = f(\alpha)$ es un homomorfismo.

Demostración:

Considerando $f(x) = a_0 + a_1 \cdot x + \dots + a_n \cdot x^n$, luego

$$\phi_\alpha(f(x)) = f(\alpha) = a_0 + a_1 \cdot \alpha + \dots + a_n \cdot \alpha^n$$

Debemos demostrar que: i) $\phi_\alpha(f(x) + g(x)) = \phi_\alpha(f(x)) + \phi_\alpha(g(x))$ e

ii) $\phi_\alpha(f(x) \cdot g(x)) = \phi_\alpha(f(x)) \cdot \phi_\alpha(g(x))$.

Esto es:

i) Se tiene que: $f(x) = \sum_{i=0}^n a_i \cdot x^i$ y $g(x) = \sum_{j=0}^m b_j \cdot x^j$

Luego $f(x) + g(x) = h(x) = c_0 + c_1 \cdot x + \dots + c_r \cdot x^r$, con $c_i = a_i + b_i$

Ahora, $\phi_\alpha(f(x) + g(x)) = \phi_\alpha(h(x)) = c_0 + c_1 \cdot \alpha + \dots + c_r \cdot \alpha^r$, con

$\phi_\alpha(f(x)) = a_0 + a_1 \cdot \alpha + \dots + a_n \cdot \alpha^n$ y $\phi_\alpha(g(x)) = b_0 + b_1 \cdot \alpha + \dots + b_m \cdot \alpha^m$, ,

es decir:

$$\begin{aligned} \phi_\alpha(f(x)) + \phi_\alpha(g(x)) &= (a_0 + a_1 \cdot \alpha + \dots + a_n \alpha^n) + (b_0 + b_1 \cdot \alpha + \dots + b_m \alpha^m) \\ &= (a_0 + b_0) + (a_1 + b_1) \cdot \alpha + \dots + (a_n + b_m) \alpha^n \\ &= c_0 + c_1 \cdot \alpha + \dots + c_r \cdot \alpha^r, \text{ con } c_i = a_i + b_i \\ &= \phi_\alpha(f(x) + g(x)) \end{aligned}$$

ii) $f(x) \cdot g(x) = \varphi(x) = d_0 + d_1 \cdot x + \dots + d_{n+m} \cdot x^{n+m}$, con $d_i = \sum_{s=0}^i d_s \cdot b_{s-i}$

luego, $\phi_\alpha(f(x) \cdot g(x)) = \phi_\alpha(\varphi(x)) = d_0 + d_1 \cdot \alpha + \dots + d_{n+m} \cdot \alpha^{n+m}$, es decir:

$$\begin{aligned} \phi_\alpha(f(x)) \cdot \phi_\alpha(g(x)) &= (a_0 + a_1 \cdot \alpha + \dots + a_n \cdot \alpha^n) \cdot (b_0 + b_1 \cdot \alpha + \dots + b_m \alpha^m) \\ &= c_0 + c_1 \cdot \alpha + c_{n+m} \cdot \alpha^{n+m}, \text{ con } c_i = \sum_{i=1}^i a_n \cdot b_{n-i} = d_i \\ &= \phi_\alpha(f(x) \cdot g(x)) \end{aligned}$$

Por lo tanto $\phi_\alpha(f(x)) \cdot \phi_\alpha(g(x)) = \phi_\alpha(f(x) \cdot g(x))$

Ejemplo 3:

Sea $\phi_0 : \mathbb{Q}[x] \rightarrow \mathbb{R}$

$$\phi_0(a_0 + a_1 \cdot x + \dots + a_n \cdot x^n) = a_0 + a_1 \cdot 0 + \dots + a_n \cdot 0^n = a_0$$

Se define: $\ker \phi_0 = \{f(x) \in \mathbb{Q}[x] / \phi_0(f(x)) = 0\}$

En el $\ker \phi_0$ están todos los polinomios sin término independiente.

Ejemplo 4:

Sea $\phi_3 : \mathbb{Q}[x] \rightarrow \mathbb{R}$

$$\text{Donde } \phi_3(a_0 + a_1 \cdot x + \dots + a_n \cdot x^n) = a_0 + a_1 \cdot 3 + a_2 \cdot 3^2 + \dots + a_n \cdot 3^n$$

$$\ker \phi_3 = \{f(x) \in \mathbb{Q}[x] / \phi_3(f(x)) = 0\}$$

Tomemos los siguientes ejemplos con $x - 3, x^2 - 9 \in \mathbb{Q}[x]$

$$\phi_3((x - 3)) = 3 - 3 = 0$$

$$\phi_3((x^2 - 9)) = 3^2 - 9 = 0$$

En el $\ker \phi_3$ están todos aquellos polinomios que tengan a 3 como raíz.

Definición 4: Si $f(\alpha) = 0$ entonces α es un cero o raíz de $f(x)$

Ejemplo 5:

Sea $f(x) = x^2 + 1 \in \mathbb{R}[x]$, ¿tiene $f(x)$ algún cero?

En los reales ($\mathbb{R}$) no posee, en cambio en los complejos ($\mathbb{C}$) si tiene, pues considerando $f(\alpha)$ tal que $\alpha = \pm i$ se tiene:

$$f(i) = i^2 + 1 = -1 + 1 = 0$$

$$f(-i) = (-i)^2 + 1 = -1 + 1 = 0$$

Ejemplo 6:

Sea $f(x) = x^3 + 2 \cdot x + 1$ en $\mathbb{Z}_3[x]$ ¿tiene $f(x)$ algún cero en $\mathbb{Z}_3$?

$$\mathbb{Z}_3 = \{0, 1, 2\}, \text{ luego } f(0) = 0^3 + 2 \cdot 0 + 1 = 1$$

$$f(1) = 1^3 + 2 \cdot 1 + 1 = 1$$

$$f(2) = 1^3 + 2 \cdot 1 + 1 = 1$$

De lo anterior podemos concluir que $f(x)$ en $\mathbb{Z}_3[x]$ no tiene cero.

Teorema: Sea K un cuerpo, entonces $K[x]$ es un Dominio Euclidiano (D.E.)

Demostración:

Debemos encontrar una función $\eta: K[x] - \{0\} \rightarrow \mathbb{Z}_0^+$ tal que:

$$i) \quad \eta(f(x) \cdot g(x)) \geq \eta(f(x))$$

ii) Sean $f(x), g(x)$ no nulos luego existen $q(x), r(x)$ tal que $f(x) = g(x) \cdot q(x) + r(x)$, con la condición que $r(x) = 0$ o $\eta(r(x)) < \eta(g(x))$

Considerando la función (grado del polinomio) $gr: K[x] - \{0\} \rightarrow \mathbb{Z}_0^+$, se tiene:

1) $gr(f(x) \cdot g(x)) \geq gr(f(x))$, en efecto:

$$gr(f(x) \cdot g(x)) = gr(f(x)) + gr(g(x)) \geq gr(f(x))$$

2) Si $f(x) = 0$ entonces $g(x) = 0$

Podemos suponer que $f(x) \neq 0$

Sea $gr(f(x)) = n$

$$gr(g(x)) = m$$

Si $n < m$, entonces $q(x) = 0$ y $r(x) = f(x)$, luego se cumple la proposición, pues $gr(f(x)) < gr(g(x))$.

Ahora si $n \geq m$

Por inducción sobre n , se tiene:

Para $n = 1$, $f(x) = a_0 + a_1 \cdot x$, con $a_1 \neq 0$ entonces $gr(g(x)) = 0$ o 1

Si $gr(g(x)) = 0$ entonces $g(x) = b_0$, luego $a_0 + a_1 \cdot x = b_0 \cdot q(x) + r(x)$

$$\text{esto es, } a_0 + a_1 \cdot x = b_0 \cdot \left(\frac{a_0}{b_0} + \frac{a_1 \cdot x}{b_0} \right)$$

Ahora si $gr(g(x)) = 1$ entonces $g(x) = b_0 + b_1 \cdot x$. Como se cumple para valores menores que n , debemos demostrar que se cumple para n .

Ahora bien, sean:

$$f(x) = a_0 + a_1 \cdot x + \dots + a_n \cdot x^n$$

$$g(x) = b_0 + b_1 \cdot x + \dots + b_m \cdot x^m$$

$$\text{Se define } F(x) = f(x) - \frac{a_n}{b_m} \cdot x^{n-m} \cdot g(x)$$

$$\text{Nota: } \frac{a_n}{b_m} \cdot x^{n-m} \cdot g(x) = \frac{a_n}{b_m} \cdot x^{n-m} \cdot (b_0 + \dots + b_m \cdot x^m)$$

Luego $F(x)$ tiene grado menor que n ; por hipótesis de inducción se tiene que existe $q_1(x)$ y $r_1(x)$ tal que $F(x) = g(x) \cdot q_1(x) + r_1(x)$ donde $r_1(x) = 0$ ó $gr(r_1(x)) < gr(g(x))$.

En efecto, $f(x) - \frac{a_n}{b_m} \cdot x^{n-m} \cdot g(x) = g(x) \cdot q_1(x) + r_1(x)$ despejando

$f(x)$ tenemos que, $f(x) = \frac{a_n}{b_m} \cdot x^{n-m} \cdot g(x) + g(x) \cdot q_1(x) + r_1(x)$, luego

$$f(x) = g(x) \cdot \left[\frac{a_n}{b_m} \cdot x^{n-m} + q_1(x) \right] + r_1(x).$$

Haciendo $\frac{a_n}{b_m} \cdot x^{n-m} + q_1(x) = q(x)$ nos resulta $f(x) = g(x) \cdot q(x) + r(x)$

donde $r(x) = 0$ ó $gr(r(x)) < gr(g(x))$.

En consecuencia $f(x), g(x) \neq 0 \in K[x]$ entonces existe $q(x), r(x)$ tal que $f(x) = g(x) \cdot q(x) + r(x)$ con $r(x) = 0$ ó $gr(r(x)) < gr(g(x))$

Observación: Es posible calcular el mcd entre $f(x), g(x) \in K[x]$.

Por el algoritmo de la división se tiene que dados $f(x), g(x) \neq 0 \in K[x]$, entonces existen $q_0(x), r_1(x)$ tal que $f(x) = g(x) \cdot q_0(x) + r_1(x)$ con $r_1(x) = 0$ ó $gr(r_1(x)) < gr(g(x))$.

Ahora si $r_1(x) = 0$ entonces $g(x)$ es el mcd entre $f(x)$ y $g(x)$

1.- $g(x) \mid f(x)$ y $g(x) \mid g(x)$

2.- Si existe $h(x)$ tal que $h(x) \mid f(x)$ y $h(x) \mid g(x)$ por demostrar $h(x) \mid g(x)$

Si $gr(r(x)) < gr(g(x))$

Usando el algoritmo de la división para $g(x)$ y $r_1(x)$, esto es existen $q_1(x), r_2(x) \in K[x]$ tal que $g(x) = r_1(x) \cdot q_1(x) + r_2(x)$, con $r_2(x) = 0$ ó $gr(r_2(x)) < gr(r_1(x))$.

Ahora si $r_2(x) = 0$ entonces $mcd(f(x), g(x)) = r_1(x)$, pues

1.- $r_1(x) | g(x)$ y $r_1(x) | f(x)$

Si $r_1(x) | g(x)$ entonces existe $s_1(x) \in K[x]$ tal que $g(x) = r_1(x) \cdot s_1(x)$

Por lo tanto $f(x) = r_1(x) \cdot s_1(x) \cdot q_0(x) + r_1(x)$.

2.- Si $h(x) | f(x)$ y $h(x) | g(x)$ por demostrar $h(x) | r_1(x)$

De 1) podemos decir que:

$$f(x) - g(x) \cdot q_0(x) = r_1(x)$$

Por lo tanto $h(x) | r_1(x)$

Ahora si $gr(r_2(x)) < gr(r_1(x))$

Por lo tanto existen $q_2(x), r_3(x) \in K[x]$ tal que $r_1(x) = r_2(x) \cdot q_2(x) + r_3(x)$

con $r_3(x) = 0$ ó $gr(r_3(x)) < gr(r_2(x))$

Ahora si $r_3(x) = 0$ entonces $mcd(f(x), g(x)) = r_2(x)$

Por otro lado si $gr(r_3(x)) < gr(r_2(x))$

Por lo tanto existen $q_3(x), r_4(x) \in K[x]$ tal que $r_2(x) = r_3(x) \cdot q_3(x) + r_4(x)$

con $r_4(x) = 0$ ó $gr(r_4(x)) < gr(r_3(x))$.

En consecuencia $r_{k-1}(x) = r_k(x) \cdot q_k(x)$ y no hay resto, pues el grado de los polinomios va disminuyendo. Por lo tanto $mcd(f(x), g(x)) = r_k(x)$.

Ejemplo 7:

Encontrar el mcd entre $f(x) = x^6 + 3x^5 + 4x^2 - 3x^2 + 2$ y $g(x) = x^2 + 2x - 3$ en $\mathbb{R}[x]$.

Trabajo previo:

$$\begin{array}{r}
 x^6 + 3x^5 + 4x^2 - 3x + 2 \div x^2 + 2x - 3 = x^4 + x^3 + x^2 + x + 5 \\
 \underline{-(x^6 + 2x^5 - 3x^4)} \\
 x^5 + 3x^4 + 4x^2 - 3x + 2 \\
 \underline{-(x^5 + 2x^4 - 3x^3)} \\
 x^4 + 3x^3 + 4x^2 - 3x + 2 \\
 \underline{-(x^4 + 2x^3 - 3x^2)} \\
 x^3 + 7x^2 - 3x + 2 \\
 \underline{-(x^3 + 2x^2 - 3x)} \\
 5x^2 + 2 \\
 \underline{-(5x^2 + 10x - 15)} \\
 17 - 10x
 \end{array}$$

Luego $f(x) = g(x) \cdot (x^4 + x^3 + x^2 + x + 5) + (17 - 10x)$

En consecuencia $g(x) = (17 - 10x) \cdot q_1(x) + r_1(x)$

Ahora determinemos $q_1(x)$ y $r_1(x)$, en efecto:

$$\begin{array}{r}
 x^2 + 2x - 3 \div -10x + 17 = -\frac{x}{10} - \frac{37}{100} \\
 \underline{-(x^2 + \frac{17x}{7})} \\
 \frac{37x}{10} - 3 \\
 \underline{-(\frac{37x}{10} - \frac{629}{100})} \\
 \frac{329}{100}
 \end{array}$$

$$\text{O sea, } x^2 + 2x - 3 = (17 - 10x) \cdot \left(-\frac{x}{10} - \frac{37}{100} \right) + \frac{329}{100}$$

Ahora, $q_2(x)$ y $r_2(x)$ están dados por:

$$-10x + 17 \div \frac{329}{100} = -\frac{1000}{329}x + \frac{1700}{329}$$

$$\begin{array}{r} -(10x) \\ +17 \\ \hline -(17) \\ 0 \end{array}$$

Luego tenemos que $17 - 10x = \left(\frac{329}{100} \right) \cdot q_2(x) + r_2(x)$, es decir,

$$17 - 10x = \left(\frac{329}{100} \right) \cdot \left(-\frac{1000}{329}x \right) + \left(\frac{1700}{329} \right)$$

$$\text{Por lo tanto el } \text{mcd}(f(x), g(x)) = \frac{329}{100}$$

Teorema del factor: Sea $f(x)$ en $K[x]$, se cumple que $f(x)$ es divisible por $(x - a)$ si y sólo si $f(a) = 0$, con a raíz del polinomio).

Demostración:

$\Rightarrow$ Hipótesis: $f(x) \in K[x]$ es divisible por $(x - a)$.

Tesis: $f(a) = 0$, con a raíz del polinomio.

Por hipótesis se tiene que $f(x) = (x - a) \cdot q(x) + r(x)$, pero como es divisible por $(x - a)$ entonces $r(x) = 0$, luego $f(x) = (x - a) \cdot q(x)$, en consecuencia $f(a) = (a - a) \cdot q(a)$, por lo tanto $f(a) = 0$.

$\Leftarrow$ Hipótesis: $f(a) = 0$, con a raíz del polinomio.

Tesis: $f(x) \in K[x]$ es divisible por $(x - a)$.

Por el algoritmo de la división, dados $f(x)$ y $(x-a)$ entonces existe $q(x)$ y $r(x)$ tal que $f(x) = (x-a) \cdot q(x) + r(x)$ con $r(x) = 0$ ó $gr(r(x)) < gr(x-a)$.

Si $r(x) = 0$ entonces $(x-a) \mid f(x)$

Ahora bien, si $gr(r(x)) = 0$ entonces $r(x) = k$, con $k \in K$, luego

$$f(x) = (x-a) \cdot q(x) + k$$

De lo anterior $f(a) = (a-a) \cdot q(x) + k$, luego $f(a) = k$, pero por hipótesis se tiene $f(a) = 0$ entonces $k = 0$, por lo tanto $f(x)$ es divisible por $(x-a)$.

En consecuencia $f(x)$ es divisible por $(x-a)$ si y solo si $f(a) = 0$.

Ejemplo 8:

Sean $f(x) = 3x^6 - 2x^4 + x^3 - x^2 + 5$, $g(x) = 2x^3 + 3x^2 - 6x + 2 \in \mathbb{Z}_7[x]$

Encuentre el *mcd* en $\mathbb{Z}_7[x]$ y expréselo como combinación lineal de $f(x)$ y $g(x)$.

$f(x) = g(x) \cdot q(x) + r(x)$, es decir:

$$3x^6 - 2x^4 + x^3 - x^2 + 5 = (2x^3 + 3x^2 - 6x + 2) \cdot (5x^3 - 4x^2 + 6x - 1) + (4x^2 - 4x)$$

$ \begin{array}{r} 3x^6 - 2x^4 + x^3 - x^2 + 5 \div 2x^3 + 3x^2 - 6x + 2 = 5x^3 - 4x^2 + 6x - 1 \\ \underline{3x^6 + x^5 - 2x^4 + 3x^3} \\ -x^5 - 2x^3 - x^2 + 5 \\ \underline{x^5 - 5x^4 + 3x^3 - x^2} \\ 5x^4 - 5x^3 + 5 \\ \underline{5x^4 + 4x^3 - x^2 + 5x} \\ -2x^3 + x^2 - 5x + 5 \\ \underline{-2x^3 - 3x^2 + 6x - 2} \\ 4x^2 - 4x \end{array} $
--

Luego $g(x) = r(x) \cdot q_1(x) + r_1(x)$, es decir:

$$2x^3 + 3x^2 - 6x + 2 = (4x^2 - 4x) \cdot (4x - 3) + (-x + 2)$$

$ \begin{array}{r} 2x^3 + 3x^2 - 6x + 2 \div 4x^2 - 4x = 4x + 3 \\ \underline{2x^3 - 2x^2} \\ 5x^2 - 6x + 2 \\ \underline{5x^2 - 5} \\ -x + 2 \end{array} $

Luego $r_1(x) = r_1(x) \cdot q_2(x) + r_2(x)$, es decir:

$$4x^2 - 4x = (-x + 2) \cdot (-4x + 3) + (-6)$$

$ \begin{array}{r} 4x^2 - 4x \div -x + 2 = -4x + 3 \\ \underline{4x^2 - x} \\ -3x \\ \underline{-3x + 6} \\ -6 \end{array} $
--

Luego $r_2(x) = r_3(x) \cdot q_4(x) + r_4(x)$, es decir:

$$-x + 2 = (-6) \cdot (6x - 5) + (0)$$

Por lo tanto $-x + 2 = -6 \cdot (6x - 5)$

En consecuencia el mcd es $-6 = \bar{1}$ en $\mathbb{Z}_7$

$ \begin{array}{r} -x + 2 \div -6 = 6x - 5 \\ \underline{-x - 5} \\ 2 \\ \underline{2} \\ 0 \end{array} $

Ejemplo 9:

Sea $f(x) = a_0 + a_1x + \dots + a_nx^n$ en $D[x]$ con D Dominio de Integridad.

Si f tiene un cero $\frac{p}{q}$ (es decir un cero racional) con $(p, q) = 1$

entonces $\frac{p}{a_0}$ y $\frac{q}{a_n}$.

Demostración:

Como $\frac{p}{q}$ es raíz de $f(x)$, entonces $f\left(\frac{p}{q}\right) = 0$, luego se tiene:

i) Dado $a_0 + a_1 \cdot \frac{p}{q} + a_2 \cdot \left(\frac{p}{q}\right)^2 + \dots + a_n \cdot \left(\frac{p}{q}\right)^n = 0$, nos resulta

$$a_0 = -a_1 \cdot \frac{p}{q} - a_2 \cdot \left(\frac{p}{q}\right)^2 - \dots - a_n \cdot \left(\frac{p}{q}\right)^n, \text{ factorizando por } p, \text{ nos queda,}$$

$$a_0 = p \cdot \left(-a_1 \cdot \frac{1}{q} - a_2 \cdot \left(\frac{1}{q}\right)^2 - \dots - a_n \cdot \left(\frac{1}{q}\right)^n \right), \text{ por lo tanto } p \mid a_0.$$

Por otro lado:

ii) Si $a_0 \cdot q^n + a_1 \cdot p \cdot q^{n-1} + \dots + a_n \cdot p^n = 0$, luego despejando nos queda

$$a_n \cdot p^n = -a_0 \cdot q^n - a_1 \cdot p \cdot q^{n-1} - \dots - a_{n-1} \cdot p^{n-1} \cdot q, \text{ para luego factorizar por } q \text{ nos resulta } a_n \cdot p^n = q \cdot (-a_0 \cdot q^{n-1} - a_1 \cdot p \cdot q^{n-2} - \dots - a_{n-1} \cdot p^{n-1}).$$

De lo anterior $q \mid a_n \cdot p^n$, pero por hipótesis se tiene que $(p, q) = 1$ luego

$q \nmid p$ por lo tanto $q \nmid p^n$, en consecuencia $q \mid a_n$.

Ejemplo 10:

Use el ejemplo anterior para encontrar los ceros racionales de

$$f(x) = 6x^4 + 17x^3 + 7x^2 + x - 10 \in \mathbb{Q}[x]$$

Si $f(x)$ tiene raíces racionales de la forma $\frac{p}{q}$ entonces $p|10$ y $q|6$

Luego $p \in \{\pm 1, \pm 2, \pm 5, \pm 10\}$ y $q \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$

Entonces $\frac{p}{q} \in \left\{ \pm 1, \pm 2, \pm 5, \pm 10, \pm \frac{1}{2}, \pm \frac{1}{3}, \pm \frac{1}{6}, \pm \frac{2}{3}, \pm \frac{5}{2}, \pm \frac{5}{6}, \pm \frac{5}{3}, \pm \frac{10}{3} \right\}$

Utilizaremos una tabla para determinar las raíces de $f(x)$, anotando en la primera fila los coeficientes del polinomio y en la primera columna sus posibles raíces.

	6	17	7	1	-10
1	6	23	30	31	21
$\frac{2}{3}$	6	21	21	15	0
$-\frac{5}{6}$	6	12	-3	$\frac{7}{2}$	$-\frac{155}{12}$

Podemos notar que $\frac{2}{3}$ es una

raíz del polinomio, por lo tanto $f(x) = \left(x - \frac{2}{3}\right) \cdot (6x^3 + 21x^2 + 21x + 15)$

Corolario: El resto al dividir $f(x)$ por $(x - a)$ es $f(a)$

Ejemplo 11:

Sea $f(x) = 2x^5 - 3x^3 + 5x^2 + x - 8$. El resto al dividir $f(x)$ por $(x + 2)$ es:

$$\begin{aligned}
 f(-2) &= 2(-2)^5 - 3(-2)^3 + 5 \cdot 2^2 - 2 - 8 \\
 &= -64 + 24 + 20 - 2 - 8 \\
 &= -30
 \end{aligned}$$

Podemos notar que el resto del polinomio es -30.

$$2x^5 - 3x^3 + 5x^2 + x - 8 \div x + 2 = 2x^4 - 4x^3 + 5x^2 - 5x + 11$$

$f(x) = 2x^5 - 3x^3 + 5x^2 + x - 8$ (unafactor más) Eduardo González, Pablo Oros & Oliver Tania (noviembre 2008)

Corolario: Un polinomio $f(x) \in K[x]$ no nulo de grado n tiene a lo más n ceros en el cuerpo K .

Demostración:

Sea a_1 un cero de $f(x)$ en K entonces $f(a_1) = 0$, luego $f(x)$ es el resto de la división de $f(x)$ por $(x - a_1)$, por lo tanto $f(x)$ es divisible por $(x - a_1)$, esto es, $f(x) = (x - a_1) \cdot q_1(x)$ donde $\text{gr}(q_1(x)) = n - 1$

Ahora, si a_2 es otro cero de $f(x)$ entonces $f(a_2) = 0$, luego $0 = f(a_2) = (a_2 - a_1) \cdot q_1(a_2)$, por lo tanto $q_1(a_2) = 0$, $q_1(x)$ es divisible por $(x - a_2)$, es decir $q_1(x) = (x - a_2) \cdot q_2(x)$ donde $\text{gr}(q_2(x)) = n - 2$.

En consecuencia $f(x) = (x - a_1) \cdot (x - a_2) \cdot q_2(x)$, como también,

$f(x) = (x - a_1) \cdot (x - a_2) \cdot \dots \cdot (x - a_r) \cdot q_r(x)$, donde $q_r(x)$ no tiene más ceros en K , por lo tanto $r \leq n$.

Si $b \in K$, con $b \neq a_i$, $\forall i = 1, r$ entonces:

$$f(b) = (b - a_1) \cdot \dots \cdot (b - a_r) \cdot q_r(b), \text{ pero } q_r(b) \neq 0, (b - a_i) \neq 0, \forall i = 1, r$$

Luego $f(b) \neq 0$, lo que significa que $f(x)$ no tiene más raíces en K .

En consecuencia $f(x) \in K[x]$ no nulo de grado n tiene a lo más n ceros en el cuerpo K .

Definición 5: Sea $f(x) \in K[x]$ un polinomio no constante. Diremos que $f(x)$ es un polinomio irreducible de $K[x]$ si $f(x)$ no puede descomponerse en el producto de dos polinomios de grado menor.

Ejemplo 12:

Sea $f(x) = x^2 - 3 \in \mathbb{Z}[x]$ es irreducible en $\mathbb{Z}$ y en $\mathbb{Q}$; pero es reducible en $\mathbb{R}$.

Propiedad: Sea $f(x)$ no constante de grado 2 o grado 3. Se tiene que $f(x) \in K[x]$ es reducible en $K[x]$ si y sólo si tiene un cero en $K[x]$.

Demostración:

$\Rightarrow$ Hipótesis: $f(x) \in K[x]$ no constante de grado 2 o grado 3 es reducible en $K[x]$.

Tesis: $f(x)$ tiene un cero en $K[x]$.

Ahora bien, si $f(x)$ es reducible en $K[x]$, entonces existe $h(x)$

, $g(x) \in K[x]$ tal que $f(x) = h(x) \cdot g(x)$ y el grado de $h(x)$ y $g(x)$ es menor que el grado de $f(x)$.

Como el grado de $f(x)$ es 2 o 3, entonces $h(x)$ o $g(x)$ es de grado 1.

Supongamos que $gr(h(x)) = 1$, entonces $h(x) = (x - a)$ (exceptuando elementos constantes de K), luego $h(a) = 0$, lo que implica que $f(a) = 0$, por lo tanto $a \in K$ es un cero de $f(x)$.

$\Leftarrow$ Hipótesis: $f(x)$ no constante de grado 2 o grado 3, tiene un cero en $K[x]$.

Tesis: $f(x) \in K[x]$ es reducible en $K[x]$.

Por otro lado sea a un cero de $f(x)$ en K , es decir $f(a) = 0$, entonces

$f(x)$ es divisible por $(x - a)$ luego $f(x) = (x - a) \cdot h(x)$, lo que implica que $gr(h(x)) = gr(f(x)) - 1$, por lo tanto $f(x)$ es reducible en K .

En consecuencia $f(x) \in K[x]$ es reducible si y sólo si tiene un cero en K .

Teorema: Sea $f(x) \in \mathbb{Z}[x]$ no constante, se cumple que $f(x)$ se factoriza en un producto de polinomios de menor grado en $\mathbb{Q}[x]$ si y sólo si se factoriza en polinomios de menor grado en $\mathbb{Z}[x]$.

Nota: Para la demostración de este teorema consulte el texto algebra abstracta de John B. Fraleigh, capítulo 31 página 283.

Corolario: Sea $f(x) \in \mathbb{Z}[x]$ con $f(x) = a_0 + a_1x + \dots + x^n$, con $a_0 \neq 0$. Si $f(x)$ tiene un cero en $\mathbb{Q}$, entonces tiene un cero m en $\mathbb{Z}$ y $m \mid a_0$.

Demostración:

Si $f(x)$ tiene un cero en $\mathbb{Q}$ entonces $f(a) = 0$, con $a \in \mathbb{Q}$, luego se tiene $f(x) = (x - a) \cdot q(x)$, con $\text{gr}(q(x)) = n - 1$ lo que significa que $f(x)$ tiene una descomposición con un factor lineal en $\mathbb{Z}[x]$.

$$f(x) = (x - m) \cdot \left(x^{n-1} + \dots + \frac{a_0}{m} \right), \quad \forall m \in \mathbb{Z}$$

Por lo tanto $\frac{a_0}{m} = k$, con $k \in \mathbb{Z}$, entonces $a_0 = m \cdot k$, en consecuencia $m \mid a_0$.

Ejemplo 13:

Sea $f(x) = x^4 - 2x^2 + 8x + 1 \in \mathbb{Q}$. Determinar si $f(x)$ es irreducible.

Suponemos que es reducible, es decir:

- i) Tiene un factor lineal
- ii) Se descompone en 2 polinomios de segundo grado.

Resolución del problema:

i) Si tiene un cero en $\mathbb{Q}$ entonces tiene un cero m en $\mathbb{Z}$ y $m|1$ entonces $m = \pm 1$, luego $f(1) = 8$ y $f(-1) = -8$;Contradicción!, pues $f(m) = 0$

Por otro lado tenemos que :

$$\begin{aligned}
 \text{ii) } f(x) &= x^4 - 2x^2 + 8x + 1 \\
 &= (x^2 + ax + b) \cdot (x^2 + cx + d) \\
 &= x^4 + ax^3 + bx^2 + cx^3 + acx^2 + bcx + dx^2 + adx + bd \\
 &= x^4 + x^3(a + c) + (b + ac + d)x^2 + (bc + ad)x + bd
 \end{aligned}$$

Por igualdad de polinomios se tiene que:

$$a + c = 0 \quad b + ac + d = -2 \quad bc + ad = 8 \quad bd = 1$$

Como $bd = 1$ entonces $b = d = 1$ o $b = d = -1$;Contradicción!, por lo tanto $f(x)$ es irreducible.

Criterio de Eisenstein: Sea p un entero primo y $f(x) = a_0 + a_1x + \dots + a_nx^n \in \mathbb{Z}[x]$ con $a_n \not\equiv 0 \pmod{p}$ pero $a_i \equiv 0 \pmod{p} \forall i < n$ y $a_0 \not\equiv 0 \pmod{p^2}$ entonces $f(x)$ es irreducible sobre $\mathbb{Q}$.

Demostración:

Por teoría anterior basta probar que $f(x)$ es irreducible en $\mathbb{Z}$.

Supongamos que f no lo es, es decir sean $g(x), q(x) \in \mathbb{Z}[x]$ tal que

$$f(x) = g(x) \cdot q(x) \text{ y } gr(g(x)) < gr(f(x)), \text{ es decir } gr(q(x)) < gr(f(x))$$

luego $f(x) = (b_r x^r + \dots + b_0) \cdot (c_s x^s + \dots + c_0)$ con $r, s < n$ y $b_r, c_s \neq 0$

es decir, $a_n x^n + \dots + a_0 = (b_r x^r + \dots + b_0) \cdot (c_s x^s + \dots + c_0)$.

Como $a_0 \not\equiv 0 \pmod{p^2}$ entonces $b_0 \cdot c_0 \not\equiv 0 \pmod{p^2}$, es decir, $b_0 \cdot c_0 \not\equiv p^2$ esto implica que b_0 y c_0 no pueden ser ambos múltiplos de p .

Supongamos que $b_0 \not\equiv 0 \pmod{p}$ y $c_0 \equiv 0 \pmod{p}$, como $a_n \not\equiv 0 \pmod{p}$ entonces $b_r \cdot c_s \not\equiv 0 \pmod{p}$, luego b_r y c_s no son múltiplos de p , es decir $b_n \not\equiv 0 \pmod{p}$ y $c_s \not\equiv 0 \pmod{p}$.

Sea m el menor valor de k tal que $c_k \not\equiv 0 \pmod{p}$, de tal forma que

$a_m = b_0 \cdot c_m + b_1 \cdot c_{m-1} + \dots + b_{m-i} \cdot c_i$, $\forall i$ con $0 \leq i < m$, luego $b_0 \cdot c_m$ no es múltiplo de p , con $b_0 \cdot c_m \not\equiv 0 \pmod{p}$, por lo tanto $a_m \not\equiv 0 \pmod{p}$, esto nos dice que $m = n$, en consecuencia $s = n$ ¡Contradicción!. Luego $f(x)$ es irreducible sobre $\mathbb{Z}$, como conclusión es irreducible sobre $\mathbb{Q}$.

Ejemplo 14:

Sea $f(x) = 25x^5 - 9x^4 + 3x^2 - 12$ es irreducible sobre $\mathbb{Q}$

Como existe $p = 3$ primo tal que $3 \nmid 25$, pero $3 \mid 9$, $3 \mid 3$, $3 \mid 12$ y $3^2 \nmid 12$

Por lo tanto $f(x)$ es irreducible sobre $\mathbb{Q}$.

Teorema (Estructura de ideal en $K[x]$): Si K es un cuerpo entonces cada ideal de $K[x]$ es principal.

Demostración:

Sea I ideal de $K[x]$, con $I = \{0\}$ entonces $I = \langle 0 \rangle$

Supongamos que $I \neq \langle 0 \rangle$, ahora bien, sea $g(x) \in I$ de grado minimal, si $gr(g(x)) = 0$ entonces $g(x) = k$, $\forall k \in K$, luego $I = K[x]$ pues, $k \in K$ es invertible, por lo tanto el ideal es $I = \langle 1 \rangle = K[x]$, o sea es todo el anillo. Por otro lado, supongamos que $gr(g(x)) \neq 0$ y sean $f(x), g(x) \in I$ por demostrar que $I = \langle g(x) \rangle$, luego por el algoritmo de la división existe $q(x), r(x)$ tal que $f(x) = g(x) \cdot q(x) + r(x)$, con $r(x) = 0$ ó $gr(r(x)) < gr(g(x))$.

Como $f(x), g(x) \in I$ entonces $r(x) \in I$ y $g(x)$ se escogió de grado minimal entonces $r(x) = 0$, por lo tanto $f(x) = g(x) \cdot q(x)$.

En consecuencia $I = \langle g(x) \rangle$. Luego cada ideal de $K[x]$ es principal.

Teorema: Un ideal $\langle p(x) \rangle \neq \{0\}$ de $K[x]$ es maximal si y sólo si $p(x)$ es irreducible sobre K .

Demostración:

$\Rightarrow$ Hipótesis: Un ideal $\langle p(x) \rangle \neq \{0\}$ de $K[x]$ es maximal.

Tesis: $p(x)$ es irreducible sobre K .

Como $\langle p(x) \rangle \neq \{0\}$ de $K[x]$ entonces $p(x)$ no es constante, luego $p(x)$ no es invertible.

Supongamos que $p(x)$ es reducible sobre K , además que existe $f(x)$ y $g(x)$ tal que $p(x) = g(x) \cdot f(x)$ con $gr(f(x)), gr(g(x)) < gr(p(x))$

Como $p(x) \in \langle p(x) \rangle$ se tiene que $g(x) \cdot f(x) \in \langle p(x) \rangle$ y como este ideal es maximal es primo entonces $g(x) \in \langle p(x) \rangle$ ó $f(x) \in \langle p(x) \rangle$.

Si $g(x) \in \langle p(x) \rangle$ entonces $g(x) = p(x) \cdot s(x)$, $\forall s(x) \in K[x]$, con $gr(p(x)) \leq gr(g(x))$ ¡Contradicción!

Ahora, si $f(x) \in \langle p(x) \rangle$ entonces $f(x) = p(x) \cdot r(x)$, $\forall r(x) \in K[x]$, con $gr(p(x)) \leq gr(r(x))$ ¡Contradicción!, por lo tanto $p(x)$ no es reducible, luego $p(x)$ es irreducible.

$\Leftarrow$ Hipótesis: $p(x)$ es irreducible sobre K .

Tesis: $\langle p(x) \rangle \neq \{0\}$ de $K[x]$ es maximal, es decir:

Sea $\langle p(x) \rangle \subset I \subset K[x]$ por demostrar $\langle p(x) \rangle = I$ ó $I = K[x]$.

Si $I \triangleleft K[x]$ entonces $I = \langle g(x) \rangle$ pero $K[x]$ es Dominio de Ideales Principales (D.I.P.)

Ahora supongamos que $\langle p(x) \rangle \neq I$ debemos demostrar que $I = K[x]$

En efecto, como $\langle p(x) \rangle \subset \langle g(x) \rangle$ luego $p(x) \in \langle g(x) \rangle$ entonces $p(x) = g(x) \cdot h(x)$, con $g(x) = \text{constante}$ ó $h(x) = \text{constante}$.

Si $g(x) = \text{constante}$ entonces $\langle g(x) \rangle = K[x]$, por lo tanto $\langle p(x) \rangle \neq \{0\}$ de $K[x]$ es maximal.

Ejemplo 15:

Demuestre que $f(x) = x^2 + 8x - 2$ es irreducible sobre $\mathbb{Q}$. ¿Es irreducible en $\mathbb{R}$, y en $\mathbb{C}$?

a) Por ver que $f(x) = x^2 + 8x - 2$ es irreducible sobre $\mathbb{Q}$.

Por criterio de Eisenstein se tiene:

Considerando $p = 2$ primo se cumple que $2 \nmid 1$ pero $2 \mid 8$, $2 \mid 2$ y $4 \nmid 2$.

Por lo tanto $f(x)$ es irreducible en $\mathbb{Q}$.

b) Por otro lado veremos si $f(x) = x^2 + 8x - 2$ es irreducible en $\mathbb{R}$ y $\mathbb{C}$.

Se tiene $x^2 + 8x - 2 = 0$, luego $x = -4 \pm 3\sqrt{2}$ lo que implica que

$x_1 = -4 - 3\sqrt{2}$ y $x_2 = -4 + 3\sqrt{2}$, por lo tanto es irreducible en $\mathbb{R}$ y $\mathbb{C}$

Ejemplo 16:

Determinar cuál de los siguientes polinomios satisface el criterio de Eisenstein.

a) $x^2 - 12$

Tomando $p = 3$ se verifica que $3 \nmid 1$ pero $3 \mid 12$ y $9 \nmid 12$, por lo tanto

$x^2 - 12$ es irreducible.

b) $4x^{10} - 9x^3 + 24x - 18$

Considerando $p = 3$ se tiene que $3 \nmid 4$ pero $3 \mid 18$, $3 \mid 24$, $3 \mid 9$ y además $9 \mid 18$

Como $9 \mid 18$, no se satisface el criterio de Eisenstein, luego

$4x^{10} - 9x^3 + 24x - 18$ no es irreducible.

Ejemplo 17:

Encuentre todos los polinomios de grado 2 que son irreducibles sobre $\mathbb{Z}_2$

Los polinomios de grado 2 podemos escribirlos como:

$$f(x) = a_2x^2 + a_1x + a_0, \text{ con } a_2, a_1, a_0 \in \mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$$

Por lo tanto $a_2=1$, luego $f(x)=x^2+a_1x+a_0$

Ahora bien, si $a_1=a_0=0$ entonces $f(x)=x^2$, es reducible, pues $f(\bar{0})=(\bar{0})^2=\bar{0}$.

Además, si $a_1=a_0=1$ entonces $f(x)=x^2+x+1$, es irreducible.

Por otro lado, si $a_1=1, a_0=0$ entonces $f(x)=x^2+x$, es reducible, pues $f(\bar{0})=(\bar{0})^2+\bar{0}=\bar{0}$.

Asimismo, si $a_1=0, a_0=1$ entonces $f(x)=x^2+1=(x+1)\cdot(x+1)$, es reducible, pues $f(\bar{0})=(\bar{1})^2+\bar{1}=\bar{0}$, está en $\mathbb{Z}_2$.

Por lo tanto el único polinomio irreducible sobre $\mathbb{Z}_2$ es $f(x)=x^2+x+1$.

Teorema: Sea $p(x)$ un polinomio irreducible en $K[x]$, si $p(x)|r(x)\cdot s(x)$, para algún $r(x), s(x)\in K[x]$ entonces $p(x)|r(x)$ ó $p(x)|s(x)$.

Demostración:

Como $p(x)|r(x)\cdot s(x)$ entonces $r(x)\cdot s(x)=p(x)\cdot q(x)$, $\forall q(x)\in K[x]$.

Luego se tiene $r(x)\cdot s(x)\in\langle p(x)\rangle$, además por hipótesis se tiene que $p(x)$ es un polinomio irreducible entonces $\langle p(x)\rangle$ es maximal, luego $\langle p(x)\rangle$ es primo, por lo tanto $r(x)\in\langle p(x)\rangle$ ó $s(x)\in\langle p(x)\rangle$, además $r(x)=p(x)\cdot q_1(x)$ ó $s(x)=p(x)\cdot q_2(x)$.

En consecuencia $p(x)|r(x)$ ó $p(x)|s(x)$.

Corolario: Si $p(x)\in K[x]$ es irreducible y $p(x)|r_1(x)\cdot\ldots\cdot r_n(x)$ $p(x)|r_i(x)$, para algún $i=1, n$

Nota: Para la demostración de este corolario consulte el texto algebra abstracta de John B. Fraleigh, capítulo 31 página 287.

Proposición: Sea $f(x)$ un polinomio no constante en $K[x]$, entonces $f(x)$ se puede factorizar en un producto de polinomios irreducibles y esta factorización es única, salvo en unidades.

Demostración:

Es evidente si consideramos a $f(x)$ irreducible.

Ahora bien, si $f(x)$ es reducible entonces $f(x) = g(x) \cdot q(x)$ tal que $gr(g(x))$ y $gr(q(x)) < gr(f(x))$, si $g(x)$ y $q(x)$ son irreducibles queda demostrado. Ahora, si alguno fuera reducible por ejemplo $g(x)$ entonces $g(x) = q_1(x) \cdot q_2(x)$, con $gr(q_1(x)), gr(q_2(x)) < gr(g(x))$, luego $f(x) = q_1(x) \cdot q_2(x) \cdot q(x)$

$\vdots$

Por lo tanto $f(x) = q_1(x) \cdot q_2(x) \cdot \dots \cdot q_r(x)$, con $q_i(x)$ irreducibles, $\forall i = 1, n$, ésta descomposición es única.

Ahora, supongamos que existen $p_i(x)$ polinomios irreducibles tal que $f(x) = p_1(x) \cdot \dots \cdot p_s(x)$ luego $p_1(x) \cdot \dots \cdot p_s(x) = q_1(x) \cdot \dots \cdot q_r(x)$, en efecto $p_1(x) \mid q_1(x) \cdot \dots \cdot q_r(x)$ lo que implica $p_1(x) \mid q_j(x)$, $\forall j = \overline{1, r}$, con $p_1(x)$ irreducible.

Supongamos que $p_1(x) \mid q_1(x)$ entonces $q_1(x) = p_1(x) \cdot h(x)$, con $q_1(x)$ irreducible, luego $h(x) = \text{constante} = u_1 \in K$, con u unidad, por lo tanto $q_1(x) = p_1(x) \cdot u_1$, en consecuencia se tiene:

$$\cancel{p_1(x)} \cdot \dots \cdot p_s(x) = \cancel{p_1(x)} \cdot u_1 \cdot q_2(x) \cdot \dots \cdot q_r(x)$$

$$p_2(x) \cdot \dots \cdot p_s(x) = u_1 \cdot q_2(x) \cdot \dots \cdot q_r(x)$$

Luego $p_2(x) \mid q_2(x) \cdot \dots \cdot q_r(x)$ entonces $p_2(x) \mid q_j(x)$, $\forall j = \overline{2, r}$

Asimismo $p_2(x) \mid q_2(x)$, por lo tanto $q_2(x) = p_2(x) \cdot u_2$, con $u_2 \in K$

En efecto, se tiene que:

$$\cancel{p_2(x)} \cdot \dots \cdot p_s(x) = u_1 \cdot u_2 \cdot \cancel{p_2(x)} \cdot q_3(x) \cdot \dots \cdot q_r(x)$$

$$p_3(x) \cdot \dots \cdot p_s(x) = u_1 \cdot u_2 \cdot q_3(x) \cdot \dots \cdot q_r(x)$$

$\vdots$

$$1 = u_1 \cdot u_2 \cdot \dots \cdot u_s \cdot (q_{s+1}(x) \cdot \dots \cdot q_r(x)), \text{ con } (q_{s+1}(x) \cdot \dots \cdot q_r(x)) = g(x)$$

Por lo tanto $r = s$, en consecuencia p_i son únicos salvo unidades,

pues $p_i(x) = u_i \cdot q_i(x)$.

Definición 6: Sea A un $D.F.U.$, diremos que un polinomio no constante $f(x) = a_0 + \dots + a_n \cdot x^n$ en $A[x]$ es primitivo si y sólo si los divisores comunes de los a_i son unidades de A .

Ejemplo 18:

Determinar si $f(x) = 3x^2 + 5x + 1$ en $\mathbb{Z}[x]$ es un polinomio primitivo.

$f(x)$ no es primitivo, pues $6x^2 + 10x + 2 = 2 \cdot (3x^2 + 5x + 1)$ y $2 \notin U(\mathbb{Z})$

Proposición: Sea A un $D.F.U.$, entonces cada polinomio no constante $f(x) \in A[x]$ se puede escribir como $f(x) = c \cdot g(x)$ donde $c \in A$ y $g(x)$ es un polinomio primitivo en $A[x]$; c y $g(x)$ son únicos salvo unidades.

Demostración:

Es evidente si $f(x)$ es primitivo.

Ahora que sucede si no lo es, sea $d = \text{mcd}(a_0, \dots, a_n)$, entonces $d \mid a_i$,

$\forall i = 0, n$, luego $a_i = d \cdot a'_i$, con $a'_i \in A$, asimismo $a_0 = d \cdot a'_0$ como también $a_n = d \cdot a'_n$, por lo tanto $f(x) = d \cdot (a'_0 + a'_1 \cdot x + \dots + a'_n \cdot x^n)$, con $d \in A$ y $(a'_0 + a'_1 \cdot x + \dots + a'_n \cdot x^n) \in A[x]$ y es primitivo.

Ahora verificaremos unicidad:

Sea $f(x) = b \cdot h(x)$, con $b \in A$ y $h(x)$ primitivo, se tiene que $f(x) = c \cdot g(x)$, considerando $e = \text{mcd}(b, c)$, podemos decir

$\frac{b}{e} \cdot h(x) = \frac{c}{e} \cdot g(x)$, con $\frac{b}{e}, \frac{c}{e} \in A$ y $\text{mcd}\left(\frac{b}{e}, \frac{c}{e}\right) = 1$, entonces

$\frac{b}{e} \cdot (b_0 + b_1 \cdot x + \dots + b_n \cdot x^n) = \frac{c}{e} \cdot (c_0 + c_1 \cdot x + \dots + c_n \cdot x^n)$, ahora, por

igualdad de polinomios se tiene:

$$\frac{b}{e} \cdot b_0 = \frac{c}{e} \cdot c_0 \quad \dots \quad \frac{b}{e} \cdot b_n = \frac{c}{e} \cdot c_n$$

Luego $\frac{c}{e} \mid \frac{b}{e} \cdot b_0$ entonces $\frac{c}{e} \mid b_0$, asimismo se verifica que $\frac{c}{e} \mid b_n$

Por lo tanto $\frac{c}{e} \mid b_i, \forall i = 0, n$, pero $h(x)$ es primitivo entonces $\frac{c}{e}$ es una unidad.

Por otra parte $\frac{b}{e} \mid c_i, \forall i=0, n$ entonces $\frac{b}{e}$ es una unidad, luego $\frac{c}{e} = u_1$, con $u_1 \in A$ unidad y $\frac{b}{e} = u_2$, con $u_2 \in A$ unidad, por lo tanto $c = e \cdot u_1$ y $b = e \cdot u_2$, con $c \cdot u_1^{-1} = e$, sustituyendo se obtiene: $b = c \cdot u_1^{-1} \cdot u_2 = c \cdot u_3$ con $u_1^{-1} \cdot u_2 = u_3$ siendo unidad en A .
Por lo tanto c y $g(x)$ son únicos salvo unidades.

Propiedad (Lema de Gauss): Sea A un Dominio de Factorización Única, entonces un producto de polinomios primitivos es primitivo.

Demostración:

Consideremos $f(x) = a_0 + a_1 \cdot x + \dots + a_n \cdot x^n$ y $g(x) = b_0 + b_1 \cdot x + \dots + b_n \cdot x^n$ primitivos en $A[x]$.

Sea $h(x) = f(x) \cdot g(x)$ y $p \in A$ un irreducible, como $f(x)$ es primitivo p no divide a todos los a_i , luego tomando a_r el primer coeficiente de $f(x)$ que no es divisible por p , es decir $p \nmid a_i, \forall i < r$.

Por otro lado como $g(x)$ es primitivo, entonces p no divide a todos los b_j . Sea b_s el primer coeficiente de $g(x)$ que no es divisible por p , es decir $p \nmid b_i, \forall j < s$.

El coeficiente de x^{r+s} en $h(x) = f(x) \cdot g(x)$ está dado por

$$c_{r+s} = a_0 \cdot b_{r+s} + a_1 \cdot b_{r+s-1} + \dots + a_{r-1} \cdot b_{s+1} + a_r \cdot b_s + a_{r+1} \cdot b_{s-1} + \dots + a_{r+s} \cdot b_0,$$

donde $a_0 \cdot b_{r+s} + a_1 \cdot b_{r+s-1} + \dots + a_{r-1} \cdot b_{s+1}$ y $a_{r+1} \cdot b_{s-1} + \dots + a_{r+s} \cdot b_0$ son

Teorema: Sea A un D.F.U., K el cuerpo de los cocientes de A , $f(x) \in A[x]$ tal que $gr(f(x)) > 0$, si $f(x)$ es irreducible en $A[x]$ entonces lo es en $K[x]$. Si $f(x)$ es primitivo en $A[x]$ e irreducible en $K[x]$, entonces $f(x)$ es irreducible en $A[x]$.

divisibles por p , pero $p \nmid a_r \cdot b_s$ entonces $p \nmid c_{r+s}$, por lo tanto $h(x)$ es primitivo.

Demostración:

$\Rightarrow$ Sea $f(x)$ un polinomio no constante en $A[x]$. Supongamos que existen $r(x), s(x) \in K[x]$ polinomios de menor grado que $f(x)$ tal que $f(x) = r(x) \cdot s(x)$.

Como $r(x), s(x) \in K[x]$, los coeficientes de estos polinomios son de la forma $\frac{a}{b}$, con $b \neq 0$ y $a, b \in A$.

Quitando denominadores se tiene que:

$$d \cdot f(x) = e \cdot r_1(x) \cdot s_1(x), \text{ con } d, e \in A,$$

$$r_1(x), s_1(x) \in A[x] \text{ y } gr(r_1(x)) = gr(r(x))$$

$$gr(s_1(x)) = gr(s(x))$$

Luego $f(x), r_1(x), s_1(x) \in A[x]$, es decir cada uno de ellos se puede escribir como el producto de un elemento de A por un polinomio primitivo en $A[x]$.

Por lo tanto se tiene que:

$$f(x) = c \cdot g(x), \text{ con } c \in A \text{ y } g(x) \text{ primitivo en } A[x]$$

$$r_1(x) = c_1 \cdot r_2(x), \text{ con } c_1 \in A \text{ y } r_2(x) \text{ primitivo en } A[x]$$

$$s_1(x) = c_2 \cdot s_2(x), \text{ con } c_2 \in A \text{ y } s_2(x) \text{ primitivo en } A[x]$$

Luego $(d \cdot c) \cdot g(x) = (e \cdot c_1 \cdot c_2) \cdot r(x) \cdot s(x)$, con $g(x), r(x) \cdot s(x)$ polinomios primitivos, entonces $(e \cdot c_1 \cdot c_2) = (d \cdot c) \cdot u$, con u unidad de A

Por lo tanto $\cancel{d} \cdot c \cdot g(x) = \cancel{d} \cdot c \cdot u \cdot r_2(x) \cdot s_2(x)$, en efecto

$c \cdot g(x) = f(x) = c \cdot u \cdot r_2(x) \cdot s_2(x)$ en $A[x]$ de lo anterior podemos decir que $f(x)$ es irreducible en $A[x]$.

$\Leftarrow$ Demostración queda de ejercicio para el lector.

Teorema: Sea A un Dominio de Factorización Única, entonces $A[x]$ también lo es.

Demostración:

Sea $f(x) \in A[x]$, con $f(x) \neq 0$ y no unidad

Si $gr(f(x)) = 0$, $f(x) = c \in A$ y como A es un D.F.U. entonces $A[x]$ también lo es.

Ahora bien, si $gr(f(x)) > 0$ entonces:

$f(x) \in K[x]$, donde K es un cuerpo de los cuocientes de A .

$f(x) = p_1(x) \cdot \dots \cdot p_r(x)$, donde $p_i(x)$ es irreducible en $K[x]$.

Los coeficientes de $p_i(x)$ son de la forma $\frac{a}{b}$, con $a, b \in A$ y $b \neq 0$

Quitando los denominadores se tiene:

$d \cdot f(x) = q_1(x) \cdot \dots \cdot q_r(x)$, donde d y los coeficientes de los $q_i(x)$ están en A , los $q_i(x)$ son irreducibles en $A[x]$ y cada $p_i(x) = q_i(x) \cdot u_i$, donde u_i es unidad de A .

Como $f(x), q_j(x) \in A[x]$, $\forall j = 1, r$ se tiene que: $f(x) = c \cdot g(x)$, con $c \in A$ y $g(x)$ primitivo en $A[x]$.

Ahora bien $q_j(x) = c_j \cdot q'_j(x)$, con $c_j \in A$ y $q'_j(x)$ primitivo en $A[x]$,

$\forall j = 1, r$, por lo tanto se obtiene que:

$d \cdot c \cdot g(x) = c_1 \cdot \dots \cdot c_r \cdot q_1'(x) \cdot \dots \cdot q_j'(x)$, entonces $c_1 \cdot \dots \cdot c_r = d \cdot c \cdot v$, donde v es unidad en A , luego sustituyendo nos resulta:

$$\cancel{d} \cdot c \cdot g(x) = \cancel{d} \cdot v \cdot q_1'(x) \cdot \dots \cdot q_j'(x), \text{ luego } f(x) = (c \cdot v) \cdot q_1'(x) \cdot \dots \cdot q_j'(x).$$

Por lo tanto $f(x)$ se descompone en producto de irreducibles en $A[x]$.

En consecuencia $A[x]$ es D.F.U.

Ejemplo 19:

Demuestre que $I = \{a + f(x) / a \in 2\mathbb{Z}, f(x) \in \mathbb{Z}[x]\}$ es un ideal de $\mathbb{Z}[x]$,

Por demostrar que, $I \triangleleft \mathbb{Z}[x]$.

Demostración:

i) Dados $a + f(x), b + g(x) \in I$ probar que $(a + f(x)) - (b + g(x)) \in I$,

tenemos que $(a + f(x)) - (b + g(x)) = (a - b) + (f(x) - g(x))$, con

$(a - b) \in 2\mathbb{Z}$ y $(f(x) - g(x)) = h(x) \in \mathbb{Z}[x]$, por lo tanto $c + h(x) \in I$.

ii) $g(x) \in \mathbb{Z}[x], a + f(x) \in I$, por demostrar que **a)** $g(x) \cdot (a + f(x)) \in I$

y **b)** $(a + f(x)) \cdot g(x) \in I$.

$$\mathbf{a)} \quad g(x) \cdot (a + f(x)) = g(x) \cdot a + g(x) \cdot f(x)$$

$$= (b_0 + b_1 \cdot x + \dots + b_n \cdot x^n) \cdot a + g(x) \cdot f(x)$$

$$= b_0 \cdot a + b_1 \cdot x \cdot a + \dots + b_n \cdot x^n \cdot a + g(x) \cdot f(x), \text{ con}$$

$b_1 \cdot x \cdot a + \dots + b_n \cdot x^n \cdot a = h(x)$, por lo tanto $b_0 \cdot a + (h(x) + f(x)) \in I$

$$\mathbf{b)} \quad (a + f(x)) \cdot g(x) = a \cdot g(x) + f(x) \cdot g(x)$$

$$= a \cdot (b_0 + b_1 \cdot x + \dots + b_n \cdot x^n) + f(x) \cdot g(x)$$

$$= a \cdot b_0 + a \cdot b_1 \cdot x + \dots + a \cdot b_n \cdot x^n + g(x) \cdot f(x), \text{ con}$$

$a \cdot b_1 \cdot x + \dots + a \cdot b_n \cdot x^n = h(x)$, por lo tanto $a \cdot b_0 + (h(x) + f(x)) \in I$

En consecuencia de lo anterior $I \triangleleft \mathbb{Z}[x]$.

Nota: A continuación se mencionarán los teoremas fundamentales de extensión a cuerpo, considerando que dichos teoremas no serán demostrados pues no forman parte esencial de nuestro estudio y se pueden desprender fácilmente de los teoremas de los capítulos anteriores.

Teorema de Kronecker: Sea F un cuerpo y sea $f(x)$ un polinomio no nulo en $F[x]$, entonces existe un cuerpo extendido E de F y un $\alpha \in E$ tal que $f(\alpha) = 0$.

Teorema: Sea K un cuerpo y I un ideal maximal de $K[x]$, entonces $K[x]/I$ es un cuerpo isomorfo a $K[\alpha]$, donde $\alpha \in E$ cuerpo, tal que $f(\alpha) \in F$.

Ejemplo 20:

Sea $\mathbb{R}$ un cuerpo y $f(x) = x^2 + 1$ un polinomio irreducible en $\mathbb{R}[x]$. El ideal $I = \langle x^2 + 1 \rangle$ es un ideal maximal de $\mathbb{R}[x]$, entonces $\mathbb{R}[x]/\langle x^2 + 1 \rangle$ es un cuerpo.

Consideremos $r \in \mathbb{R}$, con $r + \langle x^2 + 1 \rangle \in \mathbb{R}[x] / \langle x^2 + 1 \rangle$, tal que $\mathbb{R}[x] / \langle x^2 + 1 \rangle$ es un cuerpo extendido de $\mathbb{R}$.

$$\begin{aligned} \text{Si } \alpha = x + \langle x^2 + 1 \rangle, \text{ entonces } \alpha^2 + 1 &= (x + \langle x^2 + 1 \rangle)^2 + (1 + \langle x^2 + 1 \rangle) \\ &= (x^2 + 1) + \langle x^2 + 1 \rangle = 0 \end{aligned}$$

Luego α es un cero de $(x^2 + 1)$. Comúnmente se identifica $\mathbb{R}[x] / \langle x^2 + 1 \rangle$ como el cuerpo $\mathbb{C}$.

Ejemplo 21:

¿ $\mathbb{Z}_3[x] / \langle x^2 + \bar{1} \rangle$ es cuerpo?

Por teorema, $\mathbb{Z}_3[x] / \langle x^2 + \bar{1} \rangle$ es cuerpo si $\langle x^2 + \bar{1} \rangle$ es un ideal maximal.

Además se sabe que $\langle x^2 + \bar{1} \rangle$ es un ideal maximal si y sólo si $x^2 + \bar{1}$ es un polinomio irreducible en $\mathbb{Z}_3[x]$. Es claro que $g(x) = x^2 + \bar{1}$ es irreducible en $\mathbb{Z}_3[x]$, ya que para todo $\alpha \in \mathbb{Z}_3$, $g(\alpha) \neq \bar{0}$, en consecuencia $g(x) = x^2 + \bar{1}$ es irreducible en $\mathbb{Z}_3[x]$.

Por lo tanto, $\langle x^2 + \bar{1} \rangle$ es un ideal maximal de $\mathbb{Z}_3[x]$, lo que implica que $\mathbb{Z}_3[x] / \langle x^2 + \bar{1} \rangle$ es cuerpo.

Ejemplo 22:

Determine el inverso de $p(x) = \overline{(x+1)}$ en $\mathbb{Z}_{11}[x] / \langle x^2 + 1 \rangle$

Se sabe que los elementos de $\mathbb{Z}_{11}[x] / \langle x^2 + 1 \rangle$ son de la forma $\overline{(a \cdot x + b)}$, con $a, b \in \mathbb{Z}_{11}$. Si $p(x) \notin \langle x+1 \rangle$, entonces $u(x)$ tal que $u(x) \cdot p(x) = p(x) \cdot u(x) = \bar{1}$, con $p(x), u(x) \in \mathbb{Z}_{11}[x] / \langle x^2 + 1 \rangle$

Aplicando el isomorfismo de $\mathbb{Z}_{11}[x] / \langle x^2 + 1 \rangle$ en $\mathbb{Z}_{11}[\alpha]$, por el teorema

anterior y por ser φ un homomorfismo, tenemos que:

$$\varphi(u(x) \cdot p(x)) = \varphi(\bar{1})$$

$$\varphi(u(x)) \cdot \varphi(p(x)) = \varphi(\bar{1})$$

$$(a \cdot \alpha + b) \cdot (\alpha + 1) = \bar{1} + 0 \cdot \alpha$$

$$a \cdot \alpha^2 + (a + b) \cdot \alpha + b = \bar{1} + 0 \cdot \alpha.$$

Considerando que $f(\alpha) = \bar{0}$, entonces $\alpha^2 + 1 = 0$, es decir $\alpha^2 = -1$ lo que implica que $\sqrt{\alpha} = \sqrt{-1} = i$.

Luego la igualdad $a \cdot \alpha^2 + (a + b) \cdot \alpha + b = \bar{1} + 0 \cdot \alpha$ se transformará en $(a + b) \cdot \alpha + b - a = \bar{1} + 0 \cdot \alpha$, tal que se establecerán las ecuaciones:

$b - a = 1$ y $a + b = 0$. Resolviendo el sistema de ecuaciones, se tiene que las soluciones son $a = 5$ y $b = 6$.

Por lo tanto, el inverso de $p(x) = \overline{(x+1)}$ es el polinomio $u(x) = \overline{(5 \cdot x + 6)}$, tal que $p(x), u(x) \in \mathbb{Z}_{11}[x] / \langle x^2 + 1 \rangle$.

Ejemplo 23:

Determine el inverso de $p(x) = \overline{(x+1)} = (x+1) + I$ en $\mathbb{Q}[x] / \langle x^2 + 6 \cdot x + 6 \rangle$.

Primero aplicaremos el algoritmo de la división a $x^2 + 6 \cdot x + 6$ y $x + 1$, obteniendo lo siguiente:

$$\begin{array}{r} x^2 + 6 \cdot x + 6 \div x + 1 = x + 5 \\ -(x^2 + x) \\ \hline 5 \cdot x + 6 \\ -(5 \cdot x + 5) \\ \hline 1 \end{array}$$

De esta forma podemos decir que, $x^2 + 6 \cdot x + 6 = (x+1) \cdot (x+5) + 1$

, sabiendo que $\mathbb{Q}[x]$ posee estructura de cuerpo, luego despejamos el resto de la división, y obtenemos:

$$1 = x^2 + 6 \cdot x + 6 - (x+1) \cdot (x+5)$$

$$1 + I = [(x^2 + 6 \cdot x + 6) + I] - [(x+1) \cdot (x+5) + I]$$

$$1 + I = I - [(x+1) \cdot (x+5) + I]$$

$$1 + I = [(x+1) + I] \cdot [-(x+5) + I]. \quad \text{Por lo tanto, el inverso de}$$

$$p(x) = \overline{(x+1)} \text{ es el polinomio } u(x) = \overline{-(x+5)} = (x+5) + I.$$

Ejercicios

- 1.- Sea $f(x) = 1 \in A[x]$, verificar que $\phi_\alpha(f(x)) = 1$
- 2.- Sea $f(x) = x^2 - 3$, tal que $f(x) \in \mathbb{Q}[x]$, comprobar que es irreducible en $\mathbb{Q}$.
- 3.- Determinar si el polinomio $8x^3 + 6x^2 - 9x + 24$ satisface el criterio de Eisenstein.
- 4.- ¿ $\mathbb{Z}_{11}[x] / \langle x^2 + 1 \rangle$ es un cuerpo?
- 5.- ¿ $\mathbb{Q}[x] / \langle x^3 + 3 \rangle$ es cuerpo?
- 6.- Determine el inverso de $p(x) = 2 \cdot x^2 - 1$ en el cuerpo $\mathbb{Q}[x] / \langle x^3 + 3 \rangle$.
- 7.- Encuentre el número de elementos y la forma que tienen estos elementos en el cuerpo $\mathbb{Z}_3[x] / \langle x^2 + 1 \rangle$.

Desarrollo:

1.- Sea $f(x) = 1 \in A[x]$, verificar que $\phi_\alpha(f(x)) = 1$

Se tiene que:

$$\begin{aligned}\phi_\alpha(f(x)) &= \phi_\alpha(1) = \phi_\alpha(1 + a_1 \cdot x + a_2 \cdot x^2 + \dots + a_n \cdot x^n) \\ &= \phi_\alpha(1 + 0 \cdot x + 0 \cdot x^2 + \dots + 0 \cdot x^n) \\ &= 1 + 0 \cdot \alpha + 0 \cdot \alpha^2 + \dots + 0 \cdot \alpha^n \\ &= 1\end{aligned}$$

Por lo tanto $\phi_\alpha(f(x)) = 1$

2.- Sea $f(x) = x^2 - 3$, tal que $f(x) \in \mathbb{Q}[x]$, comprobar que es irreducible en $\mathbb{Q}$.

Supongamos que es reducible, entonces tiene un cero en $\mathbb{Q}$

Luego tiene un cero $m \in \mathbb{Z}$ y $m | a_0$, es decir $m | 3$

Por lo tanto $m = \pm 1$ o ± 3

Si $m = \pm 1$ entonces $f(m) = -2$

Ahora bien, si $m = \pm 3$ entonces $f(m) = 6$ ¡Contradicción!, pues $f(m) = 0$

Luego $f(x)$ es irreducible en $\mathbb{Q}$.

3.- Determinar si el polinomio $8x^3 + 6x^2 - 9x + 24$ satisface el criterio de Eisenstein.

Tomando $p = 3$ se cumple que $3 \nmid 8$ pero $3 | 24$, $3 | 9$, $3 | 6$ y $9 \nmid 24$

Por lo tanto $8x^3 + 6x^2 - 9x + 24$ es irreducible.

4.- ¿ $\mathbb{Z}_{11}[x] / \langle x^2 + 1 \rangle$ es un cuerpo?

Como se sabe por teorema, $\mathbb{Z}_{11}[x] / \langle x^2 + \bar{1} \rangle$ es cuerpo si $\langle x^2 + \bar{1} \rangle$ es un ideal maximal. Además se sabe que $\langle x^2 + \bar{1} \rangle$ es un ideal maximal si y sólo si $x^2 + \bar{1}$ es un polinomio irreducible en $\mathbb{Z}_{11}[x]$. Ahora bien, es claro que $f(x) = x^2 + \bar{1}$ es irreducible en $\mathbb{Z}_{11}[x]$, ya que para todo $\alpha \in \mathbb{Z}_{11}$ se tiene que $f(\alpha) \neq \bar{0}$, por lo tanto, de acuerdo al teorema anterior, $\mathbb{Z}_{11}[x] / \langle x^2 + \bar{1} \rangle$ es isomorfo a $\mathbb{Z}_{11}[\alpha]$.

5.- ¿ $\mathbb{Q}[x] / \langle x^3 + 3 \rangle$ es cuerpo?

Por teorema, $\mathbb{Q}[x] / \langle x^3 + 3 \rangle$ es cuerpo si $\langle x^3 + 3 \rangle$ es un ideal maximal.

Además se sabe que $\langle x^3 + 3 \rangle$ es un ideal maximal si y sólo si $x^3 + 3$ es un polinomio irreducible en $\mathbb{Q}[x]$. Es claro que $f(x) = x^3 + 3$ es irreducible en $\mathbb{Q}[x]$, por el criterio de Einseinstein:

Sea $p = 3$ tal que p es un número primo, por verificar que $p \nmid a_n$ y $p \mid a_i$ para todo $i < n$ y además $p^2 \nmid a_0$.

Es claro que $3 \nmid 1$ y $3 \mid 3$, pero $3^2 \nmid 3$ con lo cual el criterio falla, entonces $f(x) = x^3 + 3$ es irreducible en $\mathbb{Q}[x]$.

Por lo tanto, $\langle x^3 + 3 \rangle$ es un ideal maximal, lo que implica que

$\mathbb{Q}[x] / \langle x^3 + 3 \rangle$ es cuerpo.

6.- Determine el inverso de $p(x) = 2 \cdot x^2 - 1$ en el cuerpo $\mathbb{Q}[x] / \langle x^3 + 3 \rangle$.

Aplicando el isomorfismo φ de $\mathbb{Q}[x] / \langle x^3 + 3 \rangle$ en $\mathbb{Q}[\alpha]$, tenemos que

$p(\alpha) = 2 \cdot \alpha^2 - 1$. Si $p(x) \notin \langle x^3 + 3 \rangle$, entonces existe un $h(x)$ tal que

$h(x) \cdot p(x) = p(x) \cdot h(x) = \bar{1}$, con $p(x), h(x) \in \mathbb{Q}[x] / \langle x^3 + 3 \rangle$. Luego se

sabe que $h(x)$ tendrá la forma $\overline{(c \cdot x^2 + b \cdot x + a)}$. Ahora bien, aplicando el isomorfismo φ a $h(x) \cdot p(x) = \bar{1}$, se tiene que:

$$\varphi(h(x)) \cdot \varphi(p(x)) = \varphi(\bar{1})$$

$$h(a) \cdot p(a) = \bar{1}$$

$(c \cdot \alpha^2 + b \cdot \alpha + a) \cdot (2 \cdot \alpha^2 - 1) = 1 + 0 \cdot \alpha + 0 \cdot \alpha^2$, luego realizando todas las operaciones pertinentes, obtenemos la igualdad:

$$(-a - 6 \cdot b) + (-b - 6 \cdot c) \cdot \alpha + (-c + 2 \cdot c) \cdot \alpha^2 = 1 + 0 \cdot \alpha + 0 \cdot \alpha^2.$$

Ahora bien, igualando los coeficientes, obtenemos el siguiente sistema de ecuaciones $-a - 6 \cdot b = 1$, $-b - 6 \cdot c = 0$ y $-c + 2 \cdot a = 0$. Resolviendo el

sistema, tenemos como soluciones $a = \frac{1}{71}$, $b = -\frac{12}{71}$ y $c = \frac{2}{71}$.

Por lo tanto el inverso de $p(x) = 2 \cdot x^2 - 1$ es el polinomio

$$h(x) = \frac{1}{71} - \frac{12}{71} \cdot x + \frac{2}{71} \cdot x^2, \text{ tal que } p(x), h(x) \in \mathbb{Q}[x] / \langle x^3 + 3 \rangle.$$

7.- Encuentre el número de elementos y la forma que tienen estos elementos en el cuerpo $\mathbb{Z}_3[x] / \langle x^2 + \bar{1} \rangle$.

Los elementos del cuerpo $\mathbb{Z}_3[x] / \langle x^2 + \bar{1} \rangle$ son de la forma

$$f(x) + \langle x^2 + \bar{1} \rangle, \text{ donde } f(x) \in \mathbb{Z}_3[x].$$

Dados $f(x), (x^2 + \bar{1}) \in \mathbb{Z}_3[x]$, por el algoritmo de la división existen $q(x), r(x) \in \mathbb{Z}_3[x]$ tales que: $f(x) = q(x) \cdot (x^2 + \bar{1}) + r(x)$, sumando el neutro $I = \langle x^2 + \bar{1} \rangle$ del cuerpo, nos resulta:

$$f(x) + I = [q(x) \cdot (x^2 + \bar{1}) + I] + [r(x) + I]$$

$$f(x) + I = I + [r(x) + I]$$

$$f(x) + I = r(x) + I$$

Como $gr(r(x)) < gr(x^2 + \bar{1})$, lo que implica que $gr(r(x)) = 0$ o $gr(r(x)) = 1$.

(i) Si $gr(r(x)) = 0$, entonces es claro que $r(x)$ son los elementos de

$\mathbb{Z}_3$, ya que $r(x) = \sum_{i=0}^0 a_i \cdot x^i = a_0 \cdot x^0 = a_0$, con $a_i \in \mathbb{Z}_3$, luego por

definición $a_0 \in \mathbb{Z}_3$ y estarán contenidos en el cuerpo $\mathbb{Z}_3[x] / \langle x^2 + \bar{1} \rangle$.

(ii) Si $gr(r(x)) = 1$, entonces $r(x) = a \cdot x + b$, tal que $r(x) \in \mathbb{Z}_3[x]$ con

$a, b \in \mathbb{Z}_3$, de (i) e (ii), los elementos de $\mathbb{Z}_3[x] / \langle x^2 + \bar{1} \rangle$ son de la forma

$\overline{h(x)} = (a \cdot x + b) + I$ (polinomios de grado menor que el grado del polinomio generador del ideal).

Luego, como $a, b \in \mathbb{Z}_3$, podemos obtener los siguientes polinomios que se pueden visualizar en la siguiente tabla, de acuerdo a la forma $(a \cdot x + b)$ con $a, b \in \mathbb{Z}_3$:

$a \backslash b$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\overline{(x)}$	$\overline{(x+1)}$	$\overline{(x+2)}$
$\bar{2}$	$\overline{(2 \cdot x)}$	$\overline{(2 \cdot x + 1)}$	$\overline{(2 \cdot x + 2)}$

Por lo tanto el cuerpo $\mathbb{Z}_3[x] / \langle x^2 + \bar{1} \rangle$ posee 9 elementos, a saber:

$$\mathbb{Z}_3[x] / \langle x^2 + \bar{1} \rangle = \{ \bar{0}, \bar{1}, \bar{2}, \overline{(x)}, \overline{(x+1)}, \overline{(x+2)}, \overline{(2 \cdot x)}, \overline{(2 \cdot x + 1)}, \overline{(2 \cdot x + 2)} \}.$$

Autoevaluación 13

- 1.- Determine todos los polinomios irreducibles en $\mathbb{Z}_3[x]$.
- 2.- Hallar el cuociente y el resto de la división de los siguientes polinomio en $\mathbb{Q}[x]$ y luego escriba $f(x)$ usando el algoritmo de la división.
 - a) $f(x) = 5 \cdot x^6 - 3 \cdot x^3 + 18 \cdot x - 1$; $g(x) = 2 \cdot x^4 + 15 \cdot x - 3$
 - b) $f(x) = 10 \cdot x^8 - 2 \cdot x^2 + 6$; $g(x) = x^2 + 2$
- 3.- Hallar el *mcd* entre $h(x) = x^6 - 4 \cdot x^3 + 1$ y $s(x) = 3 \cdot x^2 + 5 \cdot x - 1$ tal que $h(x), s(x) \in \mathbb{Q}[x]$.
- 4.- Hallar el *mcd* entre $h(x) = x^4 + 2 \cdot x^2 + 1$ y $s(x) = x^2 + 2$ tal que $h(x), s(x) \in \mathbb{Z}_3[x]$.
- 5.- Pruebe la irreducibilidad del polinomio, $f(x) = x^3 + x + 2$ en $\mathbb{Z}_3[x]$ y en $\mathbb{Z}_5[x]$.
- 6.- ¿ $\mathbb{Z}_{11}[x] / \langle x^5 + \bar{7} \cdot x + \bar{7} \rangle$ es un cuerpo?
- 7.- Encuentre el inverso de $f(x) = 4 \cdot x + 1$ tal que $f(x) \in \mathbb{Z}_7 / \langle x^2 + 1 \rangle$.